

Published and Copyright (c) 1999 - 2013
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

<http://people.delphiforums.com/dpj/a-one.htm>
Now available:
<http://www.atarinews.org>

Visit the Atari Advantage Forum on Delphi!
<http://forums.delphiforums.com/atari/>

==~==~==

~ Six Strikes Law A Bust! ~ Web Killing Admissions? ~ Yahoo Unveils Logo!

- * Bushnell "Cynical" Over Games *-
- * Xbox One Pre-order Supply Sold Out! *-
- * Google Wants Right To Keep Scanning Gmail! *-

=~==~==

->From the Editor's Keyboard
"~~~~~"

"Saying it like it is!"

We hope that you had a terrific long Labor Day weekend!! It was quiet here, but fairly relaxing for a change. A little bit of barbecuing, as is a prerequisite for this holiday - the unofficial end of the summer. I really can't believe that we're already into September! But, there's not much that one can really do about it.

Until next time...

=~==~==

->In This Week's Gaming Section - Atari Founder 'Cynical' Over Games!
"~~~~~" Microsoft: Most Xbox One Pre-order Supply Sold Out
d Out
Microsoft Works To Save Face After Xbox Backlash!
And more!

=~==~==

->A-ONE's Game Console Industry News - The Latest Gaming News!
"~~~~~"

Microsoft Says Most Xbox One Pre-order Supply Sold Out

Retail stores in many markets have run out of Microsoft Corp's Xbox One consoles available for pre-orders, a senior company executive said, ahead of a major clash with Sony Corp's new lower-priced Playstation 4 this November.

Microsoft's first new gaming console in eight years will go on sale November 22 in 13 countries, Yusuf Mehdi, vice president of marketing, strategy and business for the Xbox, said in an interview.

That will put it one week behind the PlayStation 4 in the United States but ahead in many European countries where Sony's first new console in seven years is slated to go on sale on November 29.

The third-generation Xbox marks Microsoft's strongest push so far to dominate consumers' living rooms with an array of exclusive game and media content.

It has gone into full production and pre-orders have so far outpaced the available supply to retail stores in most markets.

"We have more pre-orders than any other Xbox console releases in history," Mehdi said, adding that the company would "enable some incremental, additional units for the day one release." He declined to give further details on the pre-orders.

The PlayStation 4, priced \$100 lower than the Xbox One at \$399, had more than 1 million pre-orders worldwide, Sony said last month.

The U.S. company is sticking to November 22 for its U.S. launch date as it is the anniversary of the 2005 launch of the Xbox 360, which helped Microsoft take the lead in the then-thriving industry. The gaming hardware industry has since lost much ground to casual gaming on smartphones and other mobile devices.

In Europe, Microsoft has struck a partnership with Electronic Arts to bundle its "FIFA 14" title from its popular soccer game franchise for free with pre-ordered consoles.

Mehdi said an upgraded Kinect motion sensor, cloud-gaming services and a lift in the consoles processing power to 1.75 gigahertz from 1.6 gigahertz would differentiate the Xbox One from its rivals.

The 13 markets set for a November launch are Australia, Austria, Brazil, Canada, France, Germany, Ireland, Italy, Mexico, Spain, the United Kingdom, the United States and New Zealand.

The launch has been delayed in some markets until 2014 to work on customizing the user interface and translating software to native languages. These markets include Belgium, Denmark, Finland, Netherlands, Norway, Russia, Sweden, and Switzerland.

Microsoft Works To Save Face After Xbox Backlash

When it comes to hyping next-generation hardware, the video game industry doesn't typically opt for simplicity. However, during a presentation at the GameStop Expo in Las Vegas to promote the upcoming Xbox One console last week, a no-frills, old-school approach is exactly what Microsoft employed when confronted with a convention room full of passionate gamers.

There were no flashy videos, sensational demonstrations or celebrity appearances. Instead, Xbox Live programming director Larry "Major Nelson" Hryb candidly took questions on stage from the crowd for 30 uninterrupted minutes, a refreshing reprieve considering the backlash Microsoft has continued to endure since unveiling the Xbox One in May.

"Look, at Xbox, we really care about the community," Hryb replied when asked point-blank how Microsoft would win back consumers. "We're very focused on what is right for gamers. Everybody at Xbox is a gamer. It's not like we just show up, do our work and go home. We want to make this the best game system that you are going to own for the next 10 years."

The presentation was apparently the first stop of an apology tour for Microsoft, which originally said the successor to the Xbox 360 would be required to go online every 24 hours and limit how users could access previously purchased games. A month later, citing feedback from consumers, Microsoft Corp. announced it decided not to implement such restrictions.

Microsoft's atypical about-face continued last month when the Redmond, Wash., company declared that an updated version of its Kinect sensor, which detects motion and voice, would no longer be required to operate the Xbox One. That turnabout came after the company, at events like the Electronic Entertainment Expo, defended how integral Kinect was to the Xbox One.

Hryb said he'll embark on a cross-country tour this month, making stops in U.S. cities to similarly assuage concerns about the next-gen console just like he did at last week's GameStop Expo. The 180-degree reversals and low-key repentance are unprecedented moves for a company like Microsoft, which once hired Cirque du Soleil to theatrically unmask the first Kinect.

Microsoft announced this week that the Xbox One will debut Nov. 22 a week after Sony Corp. unleashes its PlayStation 4 console on Nov. 14. The PS4 will cost \$399 and feature comparable computing power, high-definition graphics and online features to the Xbox One. Microsoft's console is pricier at \$499, but the system comes bundled with a Kinect sensor.

"I've pretty much made up my mind that I'm getting a PS4 and not an Xbox," said Jeff Lane, a gamer from Reno, Nev., who paid \$100 for VIP access to the GameStop Expo. "I know Microsoft has changed course on a lot of their unfounded policies since they announced the Xbox One, but what's to stop them from just implementing them next year after the console is out?"

The worries come at an important time for the gaming industry, which has seen sales slide in recent years as Microsoft's 7-year-old Xbox 360 and Sony's 6-year-old PlayStation 3 have entered their golden years. The arrival of Nintendo's Wii U last year didn't invigorate game sales, which research firm NPD Group said have dropped 9 percent over last year.

"Education is job one," said GameStop CEO Paul Raines at last week's event, which primarily served as the training grounds for the retailer's 5,000 managers. "We have thousands of people in classrooms upstairs receiving training on the Xbox One and others on the PS4. We're trying to arm our staff on how these devices will be different and how they'll work."

Raines said GameStop expects this fall's debut of the PS4 and Xbox One to make for the biggest console launch in history, while Microsoft announced that pre-orders for the third-generation Xbox have sold out faster than both the original Xbox and Xbox 360, which was released in 2005 and has been the best-selling console for the past two years.

No doubt Microsoft could use a boost to its bottom line in the coming months. The company's stock fell this week after announcing it was

spending \$7.2 billion to buy Finnish smartphone maker Nokia in an effort to better compete in the hot mobile market. And Microsoft absorbed a \$900 million charge in its last quarter to account for the flop of its Surface tablet, which runs a version of its Windows operating system.

David Wesley, author of "Innovation and Marketing in the Video Game Industry," believes Microsoft is headed in the right direction with its refocused Xbox One strategy. Wesley and other analysts don't expect the fallout from this year's botched unveiling of the Xbox One to ultimately affect sales or the public's perception of the console this holiday season.

"The reality is these concerns likely won't affect Microsoft's marketing of the Xbox One," said Wesley. "The challenge for Microsoft is conveying the value of the console without overhyping aspects that don't really meet expectations. They don't want to create such high expectations that people are letdown when the console is actually launched."

Microsoft Will Continue To Support Xbox 360 for Three More Years

Microsoft will release the Xbox One on November 22nd, but that doesn't mean the Xbox 360 will stop getting support. In fact, Xbox CMO Yusuf Medhi said during the Citi Global Technology Conference that Microsoft is shipping more games than ever and the Xbox Live subscription service is still growing. Eurogamer reports that he even went so far as to call the console incredibly profitable as it nears the last years of its life cycle.

As proof of just how much time the Xbox 360 has left, Medhi claimed that over 100 new games will ship for the 8-year-old console. Microsoft expects multiplatform games to perform very well for buyers who have yet to make the jump to the next-generation Xbox One. This is to be expected, especially considering that many of the Xbox One launch titles will also make their way to the Xbox 360.

If you look at 360 that platform lasted for seven to eight years and it's going to go for another three years, he explained. It's incredibly profitable now in the tail. Some of these things take some time in the launch year in which you invest, and then they play out over time.

Q2 2013 US Spending at \$2.88 Billion, Digital Sales Contributed \$1.77 Billion

Down 3% when compared to the \$2.97 billion spent on video game content in the United States during the second quarter of 2012, the second quarter of 2013 (April-June) saw sales of \$2.88 billion, according to a report by the NPD. When you add together spending from accessories, hardware, and total content, it actually went down 9%, which they contribute to the decline in hardware sales as we draw nearer to the PS4 launch on November 15th and Xbox One on November 22nd in the US.

For a breakdown, \$769 million was spent on new game software (including PC), \$343 million was spent on other physical forms of content (used and rental), and digital content accounted for \$1.77 billion.

Liam Callahan, Industry Analyst at The NPD Group, had this to say about the sales totals:

The decrease in new physical spending is partly due to the decline in the number of new SKU s released at retail, (with 37% fewer new SKUs in Q2 2013 compared to Q2 2012) which is to be expected as developers, publishers and consumers alike prepare for the next hardware generation. Increases in digital format spending offset nearly all the losses from the declines in physical format spending, with digital full game downloads and downloadable content spending experiencing a combined 27 percent increase (when compared to Q2 12). Spending increases occurred across both video games and PC games in the digital format.

$$= \sim = \sim = \sim =$$

```
->A-ONE Gaming Online      -      Online Users Growl & Purr!
  #####
```

Atari Founder 'Cynical' Over Games

The founder of the groundbreaking video games manufacturer Atari has said modern consoles with hefty pricetags "may be disappointing" to gamers.

Nolan Bushnell, whose Atari 2600 paved the way for cartridge plug-in games in the 1970s, said the small "incremental improvements" in consoles such as the PlayStation 4 (PS4) and Xbox One did not justify the 400 dollars (£256) they sell for.

The 70-year-old said he was "a little bit cynical" and did not believe the arguments given by modern games developers that "my photographic reality is better than your photographic reality".

He said: "I look at the games today and they're so damn good that the incremental improvement, I'm not sure is worth 400 bucks - so I think they may be disappointing."

The pioneering entrepreneur also said he feared Nintendo, whose character Super Mario has been adored by fans for decades, may be left behind in the race between the major computer games manufacturers.

While Mr Nolan praised the original Wii, he said: "I think the wii U is a terrible product, and I think Nintendo's going to be struggling."

"The standalone game systems, the handheld, I think that's over for them.

"I don't see their consoles having a significant place in the marketplace right now."

He added: "If I were Nintendo, I'd be scratching my head."

$$\begin{array}{ccccccc} \text{—} & \sim & \text{—} & \sim & \text{—} & \sim & \text{—} \end{array}$$

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Study Finds Online Privacy Concerns on the Rise

Lynn Boyden, a college professor in Los Angeles who teaches website design, says she has developed two identities online: a public one for her professional life and a private one that only a few close friends can access. She tries to block advertising trackers when she can and limits what personal data might wind up on public sites.

It's an approach that she says works, although it takes time and attention.

"It's a sliding scale," said Boyden of what information she chooses to share. "Some things are and should be private."

Americans might be sharing more personal information online than ever through social networking sites and email. But they also want to better control who can see it, according to a study released Thursday by the Pew Research Center's Internet and American Life Project.

The study reported that privacy concerns among Americans are on the rise, with 50 percent of Internet users saying they are worried about the information available about them online, up from 33 percent in 2009. Meanwhile, 86 percent of people surveyed have tried at least one technique to hide their activity online or avoid being tracked, such as clearing cookies or their browser history or using encryption.

While trying to avoid snooping at least in some circumstances is now commonplace, people cite varying reasons for doing so. About one-third said they had tried to conceal their activity from hackers or criminals, while 28 percent have tried to block advertisers. Others said they wanted to keep information private from family members or spouses, employers or the government.

"These findings reinforce the notion that privacy is not an all-or-nothing proposition for Internet users," said Mary Madden, a senior researcher at Pew. "People choose different strategies for different activities, for different content, to mask themselves from different people, at different times in their lives. What they clearly want is the power to decide who knows what about them."

Abby Drumm of Indianapolis and Dennis Wingo of Mountain View, Calif., are examples of people who want precise control over their information but for different reasons.

Drumm, a 20-year-old junior in college, said she isn't worried about advertisers or government spies digging into her digital life. She's mostly worried about offending family members. Drumm said she was confronted twice as a teenager about blog and Twitter posts that were perhaps "not family appropriate" but something she had assumed only close friends were reading.

Now, she says she has taken various steps to hide her online activity so fewer people can see what she posts or find her on various social networks.

Wingo, who owns an aerospace company, said his concern is the aggressive action being taken by the government, advertisers and hackers to invade consumers' privacy online. He says that consumers shouldn't have to opt out of advertising tracking and that businesses should pay him for anything they acquire about him online. He also says the government should have to encounter the same legal hurdles to read a person's email as it does a private letter or document inside someone's house, which isn't the case because of outdated electronic privacy laws.

"Just because we're on the Internet doesn't mean we don't have rights," Wingo said. "That's a part of public policy that has seriously lacked."

The study found that 68 percent of people agreed that the law is insufficient to protect their privacy.

Boyden agreed that more could be done to protect consumer privacy. But because the Internet is largely an unregulated global enterprise, she thinks it's probably more practical to start with educating people on basic steps they can take to protect themselves.

"There's a lot of gray area in privacy," she said. "And people's comfort levels are different."

The Pew study, done with help from Carnegie Mellon University, is based on data from 792 Internet and smartphone users contacted by telephone by Princeton Survey Research Associates International from July 11-14. The margin of error is 3.8 percentage points.

NSA Cracked Most Online Encryption

The National Security Agency, working with the British government, has secretly been unraveling encryption technology that billions of Internet users rely upon to keep their electronic messages and confidential data safe from prying eyes, according to published reports based on internal U.S. government documents.

The NSA has bypassed or altogether cracked much of the digital encryption used by businesses and everyday Web users, according to reports Thursday in The New York Times, Britain's Guardian newspaper and the nonprofit news website ProPublica. The reports describe how the NSA invested billions of dollars since 2000 to make nearly everyone's secrets available for government consumption.

In doing so, the NSA built powerful supercomputers to break encryption codes and partnered with unnamed technology companies to insert "back doors" into their software, the reports said. Such a practice would give the government access to users' digital information before it was encrypted and sent over the Internet.

"For the past decade, NSA has led an aggressive, multipronged effort to break widely used Internet encryption technologies," according to a 2010 briefing document about the NSA's accomplishments meant for its UK

counterpart, Government Communications Headquarters, or GCHQ. Security experts told the news organizations such a code-breaking practice would ultimately undermine Internet security and leave everyday Web users vulnerable to hackers.

The revelations stem from documents leaked by former NSA contractor Edward Snowden, who sought asylum in Russia this summer. His leaks, first published by the Guardian, revealed a massive effort by the U.S. government to collect and analyze all sorts of digital data that Americans send at home and around the world.

Those revelations prompted a renewed debate in the United States about the proper balance between civil liberties and keeping the country safe from terrorists. President Barack Obama said he welcomed the debate and called it "healthy for our democracy" but meanwhile criticized the leaks; the Justice Department charged Snowden under the federal Espionage Act.

Thursday's reports described how some of the NSA's "most intensive efforts" focused on Secure Sockets Layer, a type of encryption widely used on the Web by online retailers and corporate networks to secure their Internet traffic. One document said GCHQ had been trying for years to exploit traffic from popular companies like Google, Yahoo, Microsoft and Facebook.

GCHQ, they said, developed "new access opportunities" into Google's computers by 2012 but said the newly released documents didn't elaborate on how extensive the project was or what kind of data it could access.

Even though the latest document disclosures suggest the NSA is able to compromise many encryption programs, Snowden himself touted using encryption software when he first surfaced with his media revelations in June.

During a Web chat organized by the Guardian on June 17, Snowden told one questioner that "encryption works." Snowden said that "properly implemented strong crypto systems" were reliable, but he then alluded to the NSA's capability to crack tough encryption systems. "Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it," Snowden said.

It was unclear if Snowden drew a distinction between everyday encryption used on the Internet the kind described in Thursday's reports versus more-secure encryption algorithms used to store data on hard drives and often requires more processing power to break or decode. Snowden used an encrypted email account from a now-closed private email company, Lavabit, when he sent out invitations to a mid-July meeting at Moscow's Sheremetyevo International Airport.

The operator of Lavabit LLC, Ladar Levison, suspended operations of the encrypted mail service in August, citing a pending "fight in the 4th (U.S.) Circuit Court of Appeals." Levison did not explain the pressures that forced him to shut the firm down but added that "a favorable decision would allow me to resurrect Lavabit as an American company."

The government asked the news organizations not to publish their stories, saying foreign enemies would switch to new forms of communication and make it harder for the NSA to break. The organizations removed some specific details but still published the story, they said, because of the "value of a public debate regarding government actions that weaken the most powerful tools for protecting the privacy of Americans and others."

Such tensions between government officials and journalists, while not new, have become more apparent since Snowden's leaks. Last month, Guardian editor Alan Rusbridger said that British government officials came by his newspaper's London offices to destroy hard drives containing leaked information. "You've had your debate," one UK official told him. "There's no need to write any more."

Why The Latest NSA Leak Is the Scariest of All

The National Security Agency programs revealed yesterday (Sept. 5) in three media reports were perhaps the most important revelations yet this summer, and have profound implications for everyone who uses the Internet.

The reports make clear that the NSA and its British counterpart Government Communications Headquarters (GCHQ), have been methodically undermining the vast encryption-based "web of trust" that makes possible secure online financial transactions, communications and other sensitive transmissions.

The spy agencies' activities have gone on for more than a decade. Like a silent but pervasive cancer, they have penetrated and weakened every corner of the Internet.

"Not only does the worst possible hypothetical ... appear to be true," wrote Johns Hopkins cryptographer Matthew Green on his blog last night, "but it's true on a scale I couldn't even imagine."

"The companies that build and manage our Internet infrastructure, the companies that create and sell us our hardware and software, or the companies that host our data: We can no longer trust them," wrote American encryption expert Bruce Schneier on the website of the British newspaper The Guardian.

The surveillance programs, named "Manassas," "Bullrun" and "Edgehill" after battles in the American and English civil wars, not only built powerful computers to crack encryption protocols.

They also coerced technology companies into handing over encryption keys, infiltrated NSA and GCHQ personnel onto corporate staffs, broke into the computer servers of uncooperative companies to steal information and ensured that some companies built "backdoors" into their technology so that the spy agencies would always have access.

Perhaps most egregiously of all, the NSA and GCHQ deliberately poisoned publicly distributed encryption standards, used by hundreds of millions of people across the world every day, so that the standards would be secretly but fatally flawed.

"The (actually substantial) goodwill that NSA built up in the public crypto community over the last two decades was wiped out today," tweeted University of Pennsylvania cryptography expert Matt Blaze.

The implications are that, if they wanted to, the spy agencies could access nearly every Internet-based purchase, money transfer, email, Internet phone call, instant message or file transfer made by anyone, anywhere.

The programs were revealed by documents provided in June to The Guardian by former NSA contractor Edward Snowden, who has since taken refuge in Russia.

The Guardian, which has come under pressure from GCHQ to stop publishing Snowden material, shared the documents with The New York Times and the American nonprofit online outlet Pro Publica.

All three publications simultaneously posted stories on their websites yesterday afternoon.

The media outlets, wary of undermining national security in both countries, did not specify which encryption protocols have been compromised. (The spy agencies had asked that the stories not be published at all.)

But at least one has already been identified: Dual Elliptic Curve Deterministic Random Bit Generator, or Dual_EC_DRBG, a random-number generator developed by the NSA and endorsed by the U.S. federal government's National Institute of Standards and Technology (NIST) in 2007. (Random-number generators are essential to the operation of many encryption protocols.)

That same year, Schneier noted that Dual_EC_DRBG was subtly flawed in a way that permitted the holder of a secret key an unknown numerical constant to completely undermine encryption protocols based on it.

"Not only is [Dual_EC_DRBG] a mouthful to say, it's also three orders of magnitude slower than its peers. It's in the standard only because it's been championed by the NSA," Schneier wrote in a November 2007 Wired article. "We have no way of knowing whether an NSA employee working on his own came up with the constants and has the secret numbers."

Schneier, a source for some Tom's Guide articles, revealed yesterday that he has been helping The Guardian analyze the Snowden documents, and for that purpose had even bought a new computer that "has never been connected to the Internet."

"What I took away from reading the Snowden documents was that if the NSA wants in to your computer, it's in. Period," Schneier wrote in an opinion piece published on the Guardian website yesterday.

On the Guardian site, Schneier offered advice to readers seeking to keep their data private: Use the anonymizing Internet service Tor, encrypt emails and other communications and use open-source encryption software instead of commercial encryption products.

"My guess is that most encryption products from large US companies have NSA-friendly backdoors," Schneier wrote, "and many foreign ones probably do as well."

Yet even Schneier's informed recommendations may be only hopeful guesses. Because the Snowden documents did not name all the encryption protocols, pieces of software and technology companies compromised by the NSA and GCHQ, few people know what's safe and what's not.

Tor only offers partial security, and the Times' story implied that the Secure Sockets Layer (SSL) open-source security standard, which underlies nearly all secure Web transactions, had been compromised.

Likewise, the Pretty Good Privacy (PGP) open-source encryption standard, which Schneier also recommended, is so old, so widely used and was once such an irritant to the U.S. government that it would be first on a list of things for the NSA to crack.

However, just because the NSA and GCHQ could be watching you, it doesn't mean they are.

"Assume that while your computer can be compromised, it would take work and risk on the part of the NSA so it probably isn't," wrote Schneier.

It's likely some of the newer open-source technology, such as the Transport Layer Security (TLS) 1.2 Web-security standard (meant to replace SSL but not yet widely adopted), or the free RedPhone and Secure Text Android apps, are not compromised. Their code is openly available for expert review and revision.

It's also likely that closed-source technology developed by major U.S. or British corporations has been compromised. The paranoid rants dating back to the 1990s about NSA backdoors in Microsoft software or Intel chips suddenly make sense.

Even the story published last month by the German magazine Die Zeit, which suspected that Microsoft's Trusted Computing chips were secret NSA backdoors, and which we dismissed as exaggerated, no longer seems unreasonable.

"I'm no longer the crank," wrote Green on his blog yesterday, referring to his own speculation about NSA activities. "I wasn't even close to cranky enough."

The NSA and GCHQ will argue that undermining every possible piece of encryption and security is necessary for the greater good of keeping the U.S. and Britain free from terrorism, and that their adversaries in Russia and China are trying to do the same thing. (Some intelligence experts think Snowden has been a Russian agent all along.)

"Throughout history, nations have used encryption to protect their secrets, and today, terrorists, cybercriminals, human traffickers and others also use code to hide their activities," the Office of the Director of National Intelligence, James Clapper, said in a statement today (Sept. 6) and posted on Pro Publica's website. "Our intelligence community would not be doing its job if we did not try to counter that."

The fact that NSA's mission includes deciphering enciphered communications is not a secret, and is not news."

"The stories published yesterday, however, reveal specific and classified details about how we conduct this critical intelligence activity," the statement said. "Anything that yesterday's disclosures add to the ongoing public debate is outweighed by the road map they give to our adversaries about the specific techniques we are using to try to intercept their communications in our attempts to keep America and our allies safe and to provide our leaders with the information they need to make difficult and critical national security decisions."

But the collateral damage from these programs may be worse than a terrorist attack. From now on, suspicion will be cast on all products from major U.S. technology companies the key players in an industrial sector in which the U.S. is trying to maintain dominance.

Why should consumers, business or foreign governments trust software from Microsoft or McAfee, hardware from Intel or Cisco, or anything from Apple? Why buy American when cheaper Chinese products are no less secure?

A statement made a month ago by Ladar Levison, founder of the small secure email provider Lavabit, which shut down in response to government pressure, has even more resonance today.

"I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States," Levison said in a note explaining the Lavabit closure.

Google Argues for Right To Continue Scanning Gmail

Attorneys suing Google say the firm violates privacy and takes personal property by electronically scanning the contents of people's Gmail accounts and then targeting ads to them.

"This company reads, on a daily basis, every email that's submitted, and when I say read, I mean looking at every word to determine meaning," said Texas attorney Sean Rommel, who is co-counsel suing Google.

But in a federal court hearing Thursday in San Jose, Google argued that the case should be dismissed, and that "all users of email must necessarily expect that their emails will be subject to automated processing."

Judge Lucy Koh said she would consider Google's request to terminate the case, but she said she is also interested in scheduling a trial for next year, indicating she is unlikely to dismiss. She did not say when she would decide.

The lawsuit, filed on behalf of 10 individuals, is expected to be certified as a class action and is widely seen as a precedent-setting case for other email providers.

The plaintiffs say Google "unlawfully opens up, reads, and acquires the content of people's private email messages" in violation of California's privacy laws and federal wiretapping statutes. The lawsuit notes that the company even scans messages sent to any of the 425 million active Gmail users from non-Gmail users who never agreed to the company's terms.

And Rommel said "the data that's being amassed by this company" could be used for more than just targeting advertising, although the parts of the lawsuit discussing what more Google might be doing with private information is currently under seal.

"The injury is two-fold: the privacy invasion and the loss of property. Google is taking people's property because they can get it for free as opposed to paying for it," Rommel said.

Scrutinizing Google's privacy policy, Judge Koh noted that it doesn't specify that Google is scanning Gmail when it describes the type of information it's collecting.

"Why wouldn't you just say 'the content of your emails?'" she asked.

Google attorney Whitty Somvichian said that the company is attempting to have a single privacy policy for all of its services, meaning it didn't separately reference every single product.

But he said it's "inconceivable" that someone using a Gmail account would not be aware that the information in their email would be known to Google.

Google has repeatedly described how it targets its advertising based on words that show up in Gmail messages. For example, the company says if someone has received a lot of messages about photography or cameras then it might display an advertisement from a local camera store. Google says the process is fully automated, "and no humans read your email..."

"Users, while they're using their Google Gmail account, have given Google the ability to use the emails they send and receive for providing that service," Somvichian said in court. "They have not assumed the risk that Google will disclose their information and they fully retain the right to delete their emails."

Privacy advocates have long questioned the practice, and were closely watching the lawsuit.

"In this Gmail case Google is trying to argue that its technology is exempt from privacy and wiretap laws. If they win, it will set a horrible precedent that they will try to apply to other Google technologies greatly threatening consumers' privacy rights," Consumer Watchdog Privacy Project director John Simpson said on Thursday.

Former White House 'Copyright Czar' Appointed CEO of Powerful Tech Lobby Group

Victoria Espinel, who until recently served as the White House's first intellectual property enforcement coordinator, will now head one of the most powerful trade groups in the tech industry. She's been tapped to become the new president and CEO of The Software Alliance (or BSA) starting September 3rd. In her new role, she'll be tasked with pushing the anti-piracy interests of major players like Microsoft, Dell, Apple, Oracle, and Intel. And while the BSA spends a large part of its time lobbying Congress and other governments to push that agenda, Espinel will be barred from engaging in such practices herself at least initially. According to Politico, an ethics pledge Espinel took to secure her "copyright czar" position under President Obama prevents her from lobbying for at least two years.

During nearly four years at the White House, Espinel took aggressive strides to combat piracy. She coordinated with federal authorities to carry out a large number of domain seizures, effectively shutting down websites responsible for illegally streaming live sporting events and selling counterfeit drugs. She also helped craft the controversial "six-strikes" policy that has seen adoption among all major US internet providers. The rules authorize ISPs to punish users caught stealing copyrighted content with slower internet speeds or service disruptions. Those measures earned Espinel a favorable rapport with record labels, Hollywood studios, and software vendors.

But she also drew cheers among internet activists when the White House came out in opposition to the Stop Online Piracy Act (SOPA); Espinel

co-authored a letter citing the administration's concerns with the bill. President Obama has yet to fill Espinel's former role after she vacated the post two weeks ago.

Six Strikes Copyright Alert System Has Done Absolutely Nothing To Stop Piracy

After a great deal of controversy and several extensive delays, the anti-piracy Copyright Alert System was finally implemented this February for five of leading Internet service providers in the United States. And according to TorrentFreak, the program has had no noticeable effect so far. The service providers have yet to release any information about how many of their customers are receiving alerts for torrenting copyrighted material or how effective the program has been since launching six months ago, so TorrentFreak decided to resort to exterior data to determine the program's effectiveness. What follows is a graph of The Pirate Bay's traffic from the beginning of 2012 through July 2013.

If the six strikes program was working, the first logical result would be a decrease in traffic at the most visited peer-to-peer site. Instead, traffic has been trending even higher than last year, with an especially spiteful spike in March, right after the Copyright Alert System was first implemented. TorrentFreak also checked in with another popular site, ExtraTorrent, and was informed that traffic had stayed steady there as well since February. Back to the drawing board.

Erasing The Password in a Heartbeat

The Nymi is a biometric wrist band that turns the user's heart rhythm into a universal, unique authenticator for accessing everything from online banking to social media.

Created by Bionym and touted as the world's first wearable authentication device, the Nymi uses an embedded electrocardiogram sensor to monitor and recognize the wearer's heartbeat and then communicate his or her identity to a device, meaning that remembering PIN numbers and passwords could very soon be a thing of the past.

The wristband communicates information to a wirelessly connected smartphone, tablet or PC running the supporting app, essentially creating a three-factor authentication process of heartbeat, wristband and app, for the tightest security.

"When it comes to identity, privacy is a chief concern," said Karl Martin, CEO of Bionym, "The Nymi has been built by the principles of Privacy by Design. This means that each user has complete control over their data and identity. Transparency is very important to Bionym's culture, and every user has a right to know where their data is going."

At the moment, the Nymi can only be used to unlock and use electronic devices capable of running the app, the idea being that whenever a Nymi wearer sits down at their desktop or picks up their phone or even approaches their car it is unlocked and ready to go, but is inaccessible to others. But that's just the start. Bionym has also launched a Software

Developers Kit (SDK) which will enable developers to build other apps that support the technology and for companies to embed authentication via Nymi into their web services.

Interest in biometric authentication is about to explode. The next iPhone is expected to use the technology, via a fingerprint sensor in order to offer similar levels of protection while simplifying authentication, and Google has made no secret of its aims to kill off the traditional password in favor of a physical token or biometric technology. Therefore the Nymi is the first step on a journey towards the eradication of the traditional password and, hopefully, an era of safer and more secure web use.

According to a study by Nuance commissioned in May, in the US, the overwhelming majority of consumers (85%) have already lost faith in the password partly because two-thirds of web users already have 11 different usernames and passwords they need to remember. And as more and more services migrate from the physical to the virtual world, the number of passwords is growing much faster than the average person's ability to create and remember them. Little wonder that 80 percent of consumers admit to reusing and recycling the same password for multiple sites despite the security risks this entails. Therefore, the future can't come quick enough.

The Nymi is available to order now for a special price of \$79 (plus \$10 shipping to destinations beyond North America) and will ship in early 2014.

Facebook Hashtags May 'Do Nothing' To Help Promote Posts

#Bummer.

It's been several months since Facebook implemented the hashtag (#) element in its social media network, a trending topic tool first made popular by Twitter. Though the site might have originally liked the idea of piggybacking on the success of the Twitter hashtag, new data suggests that it's not quite working out that way yet.

In a recent blog post on the Facebook analytics site EdgeRank Checker, ERC employees explained that they had dug into the data to measure the impact of hashtags on Facebook's news feed and that, to their surprise, found that there was none. In fact, according to EdgeRank Checker's findings, posts with hashtags have less Viral Reach than posts without hashtags. The viral reach of posts with hashtags and those without.

EdgeRank Checker studied 500 Facebook pages in the month of July to calculate the data shown. In the over 35,000 posts by these pages, only 6,000 included hashtags. Factoring in the number of fans/friends of each page, the posts without hashtags, on average, garnered more attention by way of likes and comments.

Posts on Twitter, meanwhile, displayed an uptick in retweets when a hashtag was included, per EdgeRank Checker. For [tweets], using a hashtag typically resulted in roughly double the likelihood of being ReTweeted. Over 70% of the brands experienced an increase in RT's when using a hashtag versus not using one.

And it's not as if Twitter is the only social network to see the popularization of posts via hashtag. Instagram, a Facebook property, sees a much higher Like rate for picture posts that include a hashtag vs. those that do not, according to data put together by social media scientist and author Dan Zarrella.

So why is Facebook on the outside looking in when it comes to lucrative hashtagging? The EdgeRank Checker blog concludes that, on Facebook, Hashtags are often used in promotional material. By nature, campaigns are promotional, therefore more likely to drive less engagement, less clicks, and ultimately less Reach.

When contacted by Yahoo News, Facebook said that it's simply too early to gauge its users' temperature on hashtags.

"When we introduce a new product at Facebook, we focus on getting the user experience right; hashtags are no different," a Facebook representative told Yahoo News. Since they are prone to abuse from, for instance, meme Pages, we've been focused on fine tuning the ranking algorithms before we surface them more prominently to people.

In addition, Facebook seems to think that, at least for now, the quality of posts is more important than simple hashtag placement, explaining that, Pages should not expect to get increased distribution (what some call virality) simply by sticking irrelevant hashtags in their posts.

As Facebook, Instagram and Twitter are clearly different animals, should we expect the device to play the same role across all social network platforms? At least for now, the answer seems to be #no.

Patriots Deploy Free Stadium-wide Wi-Fi To Compete with the Comforts of Home

Nothing can replace watching a sports game at the local stadium except for HD TVs, warm living rooms and nearby snacks. A recent ESPN poll found that 41 percent of fans would rather watch a game at home than at a stadium.

You have your own bathroom, the fridge is 10 feet away and the cost of a big-screen TV is less than it ever was, says Fred Kirsch, publisher and VP of content at the New England Patriots football franchise. Those are really hard to compete with.

But the Patriots are hoping to do just that by rolling out free Wi-Fi at Gillette Stadium this season to give fans a more connected experience at the team's eight home games. NFL Commissioner Roger Goodell endorsed this idea in May, saying every NFL stadium should have high-speed Wi-Fi for its fans.

Too many stadium selfies for cellular networks

The Patriots stadium used to rely on cellphone networks for mobile traffic, but that approach couldn't handle the large number of photo uploads and status updates fans transmitted during games.

After piloting Wi-Fi in 2012, the team and networking vendor Enterasys are rolling it out in full for the upcoming 2013-14 football season. The network will have 360 access points and enough bandwidth to handle at least 16,000 concurrent users.

"The app will include live play-by-play, bathroom wait times, a tool for ordering concessions from your seat, and access to NFL RedZone."

Along with the Wi-Fi network, the Patriots developed a mobile app called Patriots Game Day Live, available to anyone attending a game at Gillette Stadium. The team tested a version of the app last season with fans in luxury club seats and although only 10 percent of those fans used it, Kirsch says the team hopes to see that number increase by offering content that is only available through the app.

We are trying to give things here that you can't get in your living room, he says.

The app will include live play-by-play, bathroom wait times, a tool for ordering concessions from your seat, and access to NFL RedZone, a live compilation of all the scoring plays from games around the league.

The Wi-Fi network is expected to allow 40 percent of the 70,000 fans in the stadium to connect simultaneously. Kirsch says that, down the line, the team hopes to add unique content such as audio from players wearing microphones and video from the sidelines or locker room.

Yahoo Unveils New Logo in Turnaround Makeover

Yahoo has refreshed its logo for the first time since shortly after the Internet company's founding 18 years ago.

The new look unveiled late Wednesday is part of a makeover that Yahoo Inc. has been undergoing since the Sunnyvale, Calif., company hired Google executive Marissa Mayer to become Yahoo's CEO 14 months ago.

Mayer has already spruced up Yahoo's front page, email and Flickr photo-sharing service, as well as engineered a series of acquisitions aimed at attracting more traffic on mobile devices. The shopping spree has been highlighted by Yahoo's \$1.1 billion purchase of Tumblr, an Internet blogging service where the company rolled out its new logo.

The redesigned logo retains some of the elements of the old one, including the company's official color, purple. Yahoo's familiar exclamation point, meant to punctuate a yodeling sound that has long been the company's calling card, is still there, too, but with a twist. When visitors come to Yahoo's front page or an app, the exclamation point dances across some of the lettering before settling at the end of the company's name at a slight tilt of nine degrees.

"We knew we wanted a logo that reflected Yahoo whimsical, yet sophisticated," Mayer wrote on her Tumblr account. She hailed the redesigned looks as "modern and fresh, with a nod to our history. Having a human touch, personal. Proud."

Mayer, 38, said she spent most of one weekend this summer figuring out what the new logo should look like with four other Yahoo colleagues: Bob Stohrer, Marc DeBartolomeis, Russ Khaydarov, and an intern, Max Ma.

In an effort to drum up more interest in the changeover, Yahoo spent the past 30 days showing some of the proposed logos that Mayer and her helpers cast aside.

The revision is the first time that Yahoo has made a significant change to its logo since a few tweaks shortly after co-founders Jerry Yang and David Filo incorporated the company in 1995.

Since Yahoo's logo is so recognizable, it's a good thing they kept the changes relatively sedate, says branding expert Laura Ries, of the Atlanta firm Ries & Ries.

"One of the worst things in the world you can do is have a logo around for two decades and then do something totally different. It's quite unsettling for consumers," she said. Keeping the purple and the exclamation point was a good idea, she said.

Mayer's overhaul of Yahoo has attracted a lot of attention, but so far it hasn't provided a significant lift to the company's revenue. Yahoo depends on Internet advertising to make most of its money, an area where the company's growth has been anemic while more marketing dollars flow to rivals such as Google Inc. and Facebook Inc.

A new logo is an important part of updating Yahoo, Ries said, but at the end of the day the company has to do a better job of "verbalizing what exactly Yahoo is."

"There's nothing wrong with improving something, putting lipstick on something, but at the end of the day is it a pig or not? That is the question," Ries said.

Yahoo's stock has climbed by nearly 80 percent, but most of that gain has been driven by the company's 24 percent stake in China's Alibaba Holdings Group. Investors prize Alibaba because it has emerged as one of the fastest growing companies on the Internet.

How The Internet Is Killing The Dreaded Admissions Essay

Five years ago, Tufts University was among the first higher-education institutions to accept short-form videos, perhaps shared with the school via YouTube, as an alternative or addition to a written application essay. Lee Coffin, the school's dean of undergraduate admissions, recalls that there was some drop-jawed skepticism about the legitimacy of this option at the time: To some the notion sounded not only less than credible, but downright silly.

But in 2013, it seems clear that technology shifts are reshaping the parameters of venerable admissions rituals at many schools. George Mason, William and Mary, and St. Mary's College of Maryland have all accepted video and multimedia materials; traditional essay-question prompts are changing to reflect the reality of Internet culture. The University of Virginia this year asks: To tweet or not to tweet? MIT recently heralded the opening of its current online application form with some snappy GIFs. And applicants to Tufts grappled with a question linking the ancient Roman notion of *carpe diem* with a more contemporary idea: What does #YOLO mean to you?

Of course, the intersection of Web culture and higher ed aspirations hasn't always been pretty. The discovery of a Google doc collection of Columbia University application essays became fodder for Gawker snark.

And arguably the most viral bit of college-admission content ever was an op-ed earlier this year from a high schooler complaining about (or lampooning) the gap between university and applicant expectations.

The whole notion of new media incursion into the staid realm of the application essay may sound a little fishy to you. But the reality is almost exactly the opposite of the knee-jerk stereotype.

The influence of technology on the application process is more subtle; nobody is getting into a school because of a good tweet. The University of Chicago uses its alumni and student email networks, for example, to crowdsource its famously clever essay prompts. And the vast majority of applicants even to new-media-friendly schools still opt for the traditional written essay. And that's fine, says Tufts' Coffin. The point isn't to force potential students to play by a new set of rules, let alone provide them techno-shortcuts. The point is to acknowledge that there is more than one way to identify promising students.

Interestingly, Coffin says that at Tufts the decision to accept video or Web-based material had decidedly analog roots. Some years ago, Robert Sternberg, then the school's dean of arts and sciences, pushed for new ways of exploring conceptions of merit among applicants by including in the admissions process a challenge to do something with an 8X11 piece of paper. This experiment yielded compelling responses from art, architecture, and theater hopefuls that demonstrated demonstrations of student merit that you don't necessarily capture if you only let them write an essay, Coffin recalls.

Building on that insight is what led to trying out videos and other Web-based material not as a replacement to essays, but as an option. And as it happens, this more tech-forward approach played into broader trends.

It seemed consistent with the way teachers are developing their curriculums in high school, Coffin adds. The pedagogy has shifted; it's not just a chalkboard anymore.

The mere willingness to accept new-media application material, assistant director of admissions Justin Pike suggests, bolsters Tufts' image as a school that's in tune with the Internet era: Even students who submit traditional essays often note their appreciation of the school's recognition of new-media alternatives as perfectly legitimate.

And that was true even back in 2009, when Betty Quinn was among the earlier Tufts aspirants to supplement her application with an impressive stop-motion video which racked up tens of thousands of views as a result of media coverage at the time. Turns out that while then-Virginia-resident Quinn was accepted, she ended up going to the University of Virginia.

But from what she told me recently, making that video for Tufts seems to have had a much more lasting effect than most essay-writing exercises do. At the time she was thinking of pursuing a journalism or pre-med degree, and had never made a video. Telling my story in a completely different media was an eye-opener, she recalls, and ultimately she shifted her focus to the creative side of marketing, particularly film, animation, and interaction design; today she's in grad school at Parsons. And people still randomly bring up her Tufts video.

I loved the entire process, she says now and when you consider that she's talking about the process of applying to college, that's a pretty

remarkable statement.

==~==~==

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.